FY 2017 ANNUAL REPORT TO CONGRESS:

E-GOVERNMENT ACT IMPLEMENTATION

OFFICE OF MANAGEMENT AND BUDGET

March 2018

TABLE OF CONTENTS

INTRODUCTION

Since the passage of the E-Government Act of 2002 (E-Gov Act) 44 U.S.C. § 3601, Federal agencies have made significant progress in using the internet and other technologies to enhance citizen access to Government information and services, thereby improving Government transparency, data-driven decision making and the customer experience . The E-Gov Act requires Federal agencies and the Office of Management and Budget (OMB) to report annually on their progress implementing the various provisions of the E-Gov Act, as described in more detail below.

OMB developed this report in accordance with 44 U.S.C. § 3606, which requires OMB to provide a summary of the information reported by Federal agencies and a description of compliance by the Federal Government with the provisions of the E-Gov Act. The E-Gov Act includes numerous requirements for OMB and Federal agencies to ensure effective implementation. For example, the E-Gov Act requires agencies to provide OMB links to various websites including the agency's Freedom of Information Act (FOIA) information and agency activities on www.USA.gov. This report provides a summary of OMB and agency compliance with these requirements. Additionally, in an effort to streamline this year's report, OMB has utilized the Federal IT Dashboard (IT Dashboard) to provide agency implementation data. The information on the IT Dashboard reflects agency submissions provided to OMB.

Additionally, consistent with previous E-Gov Act reports, this report includes information required under the Federal Funding Accountability and Transparency Act of 2006 (Pub. L. No. 109-282, codified at 31 U.S.C. § 6101 note). Under this Act, OMB is required to oversee and report to Congress on the development of a website through which the public can readily access information about grants and contracts provided by the Federal agencies.[1]

This report is structured in numerical order according to the required sections of the E-Gov Act. For a description of reporting requirements and the corresponding report sections, please see Appendix I. This report is organized as follows:

- **Section I – Office of E-Government Initiatives**
  In accordance with Section 101 of the E-Gov Act (44 U.S.C. §§ 3604 and 3606), this section describes the status of the E-Government Fund (E-Gov Fund) in Fiscal Year (FY) 2017. Since FY 2015, appropriations for the E-Gov Fund have been appropriated to the General Services Administration's (GSA) Federal Citizen Services Fund (FCSF). Any remaining balances in the E-Gov Fund were authorized to be transferred to the FCSF. This section describes some of the initiatives that the Office of the Federal Chief Information Officer (OFCIO) (formerly the Office of Electronic Government and IT)

[1] Federal Funding Accountability and Transparency Act of 2006, 31 U.S.C. § 6101 note provides:

REPORT.— (1) IN GENERAL.—The Director of the Office of Management and Budget shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Government Reform of the House of Representatives an annual report regarding the implementation of the website established under this section. (2) CONTENTS.—Each report submitted under paragraph (1) shall include—(A) data regarding the usage and public feedback on the utility of the site (including recommendations for improving data quality and collection); (B) an assessment of the reporting burden placed on Federal award and subaward recipients; and (C) an explanation of any extension of the subaward reporting deadline under subsection (d)(2)(B), if applicable. (3) PUBLICATION.—The Director of the Office of Management and Budget shall make each report submitted under paragraph (1) publicly available on the website established under this section.

leads to improve the transparency, efficiency, and effectiveness of Federal operations, and increase citizen participation in Government.

- **Section II – Government-wide Information Technology (IT) Workforce and Training Policies**
  In accordance with Section 209 of the E-Gov Act (44 U.S.C. § 3501 note), this section provides a summary of activities related to IT workforce policies, evaluation, training, and competency assessments.

- **Section III – Disaster Preparedness**
  In accordance with Section 214 of the E-Gov Act (44 U.S.C. § 3501 note), this section provides a summary of how IT is used to further the goal of maximizing the utility of IT in disaster management.

- **Section IV – Geospatial**
  In accordance with Section 216 of the E-Gov Act (44 U.S.C. § 3501 note), this section provides a summary of activities on geospatial information systems and initiatives and an overview of the Geospatial Platform.

- **Appendices – Compliance with Other Goals and Provisions of the E-Gov Act**
  The appendices contain broad overviews of activities agencies are undertaking to comply with the goals of the E-Gov Act, including highlights of some agency-specific efforts. Full agency descriptions of compliance with each provision of the Act can be found on the IT Dashboard. As part of the broader OMB effort to eliminate duplicative data collections and reduce reporting burden placed on Federal agencies, OMB did not request information for several appendices in its annual E-Gov Act implementation data collection this year. Specifically, information was not collected from agencies that in past reports would have been included in Appendix D, Appendix E, Appendix F, and Appendix G. Please read explanations in each of these sections noting primary sources where this information can be found.

    - *Appendix A - Enhanced Delivery of Information and Services to the Public:* In accordance with Section 101 of the E-Gov Act, (44 U.S.C. § 3602(f)(9)), this appendix describes agency activities that enhance delivery of information and services to the public.

    - *Appendix B - Performance Integration:* In accordance with Section 202(b) of the E-Gov Act (44 U.S.C. § 3501 note), this appendix describes performance metrics being used and tracked for IT investments, and how these metrics support agencies' strategic goals and statutory mandates.

    - *Appendix C - Government-Public Collaboration:* In accordance with Section 202(e) of the E-Gov Act (44 U.S.C. § 3501 note), this appendix describes how agencies utilize technology to initiate Government-public collaboration in the development and implementation of policies and programs.

- *Appendix D - Credentialing:* In accordance with Section 203 of the E-Gov Act (44 U.S.C. § 3501 note), this appendix describes current activities agencies are undertaking to achieve interoperable implementation of electronic credential authentication for Federal Government transactions. In an effort to eliminate duplicative data collections and reduce reporting burden on agencies, information for this appendix was not collected this year. For information on agency initiatives in implementing security standards, including the adoption of PIV cards, please see OMB's FY17 FISMA Report

Commented [MZTE(1]: Link once the FY17 report is released.

- *Appendix E - E-Rulemaking:* In accordance with Section 206 of the E-Gov Act (44 U.S.C. § 3501 note), this appendix describes agencies' online electronic regulatory submission capabilities, specifically the usage of www.Regulations.gov and the Federal Docket Management System. In an effort to eliminate duplicative data collections and reduce reporting burden on agencies, information for this appendix was not collected this year. To view proposed rules, requests for information, or other documents that Federal agencies have issued for public feedback, please view the Regulations.gov or FDMS websites.

- *Appendix F - National Archives Records Administration Recordkeeping:* In accordance with Section 207(d) and (e) of the E-Gov Act (44 U.S.C. § 3501 note), this appendix describes agencies' adherence to the National Archives and Records Administration's recordkeeping policies and procedures for electronic information online and other electronic records. In an effort to eliminate duplicative data collections and reduce reporting burden on agencies, information for this appendix was not collected this year. To view NARA's record of agency inspections, records management program reviews, surveys and assessments, and annual reporting, please review the Records Management Oversight and Reporting Program's website.

- *Appendix G – Privacy Policy and Privacy Impact Assessments:* In accordance with Section 208(b) of the E-Gov Act (44 U.S.C. § 3501 note), this appendix provides information regarding agencies' privacy impact assessments and privacy policies. In an effort to eliminate duplicative data collections and reduce reporting burden on agencies, information for this appendix was not collected this year. For information on agency privacy initiatives, please see OMB's FY17 FISMA Report

Commented [MZTE(2]: Link once the FY17 report is released.

- *Appendix H - Agency Information Technology Training Programs:* In accordance with Section 209(b) of the E-Gov Act (44 U.S.C. § 3501 note), the appendix describes agency training programs for the IT workforce.

- *Appendix I - Description of E-Gov Act Reporting Requirements and Corresponding Report Sections.*

SECTION I: OFFICE OF E-GOVERNMENT INITIATIVES

The E-Government Fund

The E-Gov Act established an E-Gov Fund to provide financial support for the innovative use of IT in the Federal Government (44 U.S.C. § 3604). Projects supported by the E-Gov Fund included efforts to:

- Make Federal Government information and services more readily available to members of the public;
- Make it easier for the public to apply for benefits, receive services, pursue business opportunities, submit information, and otherwise conduct transactions with the Federal Government; and
- Enable Federal agencies to take advantage of IT in sharing information and conducting transactions with each other and with state and local governments.

Pursuant to the Act, OMB was required to report annually to Congress on the operation of the Fund, including which projects the Director of OMB approved for funding from the Fund, and the results those funded projects that achieved.

Since FY 2015, as first specified in the Consolidated and Further Continuing Appropriations Act 2015, Pub. L. No. 113-235, funding for E-Gov Act projects has been appropriated to the GSA Federal Citizen Services Fund (FCSF) rather than to the E-Gov Fund. Therefore, GSA's FCSF now manages the allocation of funds to support E-Gov Act IT initiatives. The 2015 Appropriations Act also permitted transfer of any funds in the E-Gov Fund from fiscal years prior to FY 2015 that remained unobligated as of September 30, 2014, to the FCSF.[2]

[2] Consolidated and Further Continuing Appropriations Act 2015, Pub. L. No. 113-235 https://www.gpo.gov/fdsys/pkg/PLAW-113publ235/html/PLAW-113publ235.htm

Select Highlights of OFCIO Initiatives for FY 17

The Office of E-Gov (OFCIO) at OMB continues to drive innovation in Government operations, using IT to improve the transparency, efficiency and effectiveness of Federal operations, and increase citizen participation in Government.

Data Center Optimization Initiative & Cloud Strategy

In 2010, OMB launched the Federal Data Center Consolidation Initiative (FDCCI) to reduce the number of Federal data centers and associated costs. Even with those initial efforts, by 2014 more than 9,000 data centers remained in the Federal inventory. As a result, Congress passed the Federal Information Technology Acquisition Reform Act (FITARA) in 2014, which required OMB to release updated guidance for agencies on data center optimization. OMB issued FITARA implementation guidance for agencies in OMB memorandum M-15-14: *Management and Oversight of Federal Information Technology* (listed on management.cio.gov). OMB also released a new data center strategy, M-16-19: *Data Center Optimization Initiative* (DCOI) on August 1, 2016, which set a goal of closing approximately 52% of the remaining 9,000 data centers in the Federal inventory. The initiative also seeks to optimize remaining data centers across five metrics, develop a shared services marketplace in conjunction with the General Services Administration (GSA), and reduce data center spending by $2.7 billion by the end of FY 2018. OMB then worked with the CIO Council to set up a magnagement.cio.gov page to provide additional information to assist agencies in meeting their closure goals. Since implementation of DCOI, agencies have closed an additional 2,926 data centers, resulting in more than $3 billion in report cost savings and avoidances across the Federal Government. OMB continues to assist agencies with oversight and implementation support for the DCOI goals. The latest DCOI cost-savings, closures, and optimization figures are all available on the IT Dashboard.

DCOI will sunset at the end of the FY 2018, thus requiring a new policy to update agency metrics, milestones, and reporting requirements. The IT Modernization Report, a document created in response to Executive Order (EO) 13,800 also includes a milestone to update OMB's Cloud First policy. More information will be included in the next annual report to describe progress made towards this initiative.

Cybersecurity Efforts

In accordance with the Federal Information Security Modernization Act of 2014 (FISMA), OMB is responsible for overseeing Federal agencies' information security practices and developing and implementing related policies and guidelines. The Federal Chief Information Security Officer (CISO) leads the OMB Cyber and National Security Unit (OMB Cyber), which serves as the dedicated team within OFCIO that works with Federal agency leadership to address information security priorities. OMB Cyber collaborates with partners across the Government to develop cybersecurity policies, conduct data-driven oversight of agency cybersecurity programs, and coordinate the Federal response to cyber incidents.

During FY 2017, Federal agencies made considerable progress in strengthening their

defenses and enhancing their workforces to combat cyber threats. In particular, agencies worked to enforce the use of multi-factor Personal Identity Verification (PIV) cards, with 88% of Government users now using this credential to access Federal networks. Additionally, all civilian CFO Act agencies now meet Federal anti-phishing targets, with 19 also meeting Federal malware defense targets. Agencies have also made significant progress toward safeguarding their high value IT assets and employing capabilities to identify, detect, and protect hardware and software assets on their networks.

OMB also worked to implement Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Pursuant to this effort, OMB assessed 96 agencies to determine the level to which they were actively managing their cybersecurity risk. Not only was this the largest assessment of Federal agencies to have been undertaken, the use of over 70 metrics also marks the most in-depth assessment of Federal cybersecurity thus far carried out. This information informed the Federal Cybersecurity Risk Determination Report and Action Plan to the President of the United States, which set forth OMB's findings and provided recommendations to the President for improving the state of Federal cybersecurity.

The Executive Order 13800 also tasked the Director of the American Technology Council (ATC) to coordinate a report to the President regarding the modernization of Federal IT. The resulting Report to the President on Federal IT Modernization describes the need to embrace the broader use of cloud and shared services, while collecting agency data to help inform the actions described in the report.

Additional information about these efforts can be found in the FY 2017 Annual FISMA Report.[3]

Commented [OMB3]: We can update with a link once we have one.

Open Government and Federal Source Code

In FY 2017, the Interagency Open Data Working Group continued to responsibly present the power of data for the benefit of the American public and maximize the nation's return on its investment in data. Led by OMB and the Data.gov team at the GSA, this community of practice hosts monthly implementation meetings on Project Open Data for Federal employees and contractors. It connects over 900 Federal data professionals who develop open data tools share best practices, and ensure the adoption of best practices related to data governance, data policy, and the hiring and training of data science professionals. These U.S. Government Open Data meetings are open to public stakeholders on a quarterly basis.

Also in FY 2017, OFCIO led OMB initiatives to prioritize agile development with users and emerging technologies to further facilitate the release of open data. OMB, GSA Data.gov, and GSA DigitalGov teams worked with Federal agencies to promote consistent, customer-friendly feedback mechanisms on opening new datasets and improving existing datasets to fuel innovation and real-world impact through data-driven government. Data.gov is home to the Federal Government's open data, where the public can search nearly 200,000 Government

[3] Link to FY17 FISMA Report

datasets, tools, and resources to conduct research, develop web and mobile applications, design data visualizations, which helps fuel American innovation, entrepreneurship, businesses, and more. Project Open Data provides agencies with tools and best practices to make their data publicly available. Project Open Data Dashboard provides publicly accessible evaluations of agency progress in implementation of OMB memorandum M-13-13: *Open Data Policy—Managing Information as an Asset*. OMB continues to update the agency evaluations on a quarterly basis.

In May 2017 the Treasury Department, in a collaboration with OMB to advance Open Government/Data, released the new version of the USAspending.gov site in accordance with the Digital Accountability and Transparency Act (DATA Act) requirements. The "Beta" site will run concurrently with the previous version of the Beta.USAspending.gov website over the summer to minimize disruptions to users' data access and provide more time to add user-centered enhancements. The new Beta.USAspending.gov site tracks agency expenditures and for the first time, links relevant agency expenditure data with awards distributed by the Government.

In the FY16 E-Gov Act Report, OMB first described its successful release of OMB memorandum M-16-21: *Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software*. This policy aimed to mitigate wasteful spending associated with duplicative software acquisitions, ultimately reducing the $6 billion that the Federal Government spends each year on new software transactions. Following this policy, new custom software developed specifically for or by the Federal Government must be made available for sharing and reuse across all Federal agencies. This has the potential to save significant taxpayer dollars by trimming duplicative acquisitions and avoiding vendor lock-in. In addition, agencies are required to take part in an open source pilot program. Agencies will share 20 percent of new federally funded custom code as open source software as part of a three-year pilot program designed to maximize the economic benefits associated with code sharing and reuse. This portion of the policy will sunset after three years.

In November 2016, OMB launched Code.gov to facilitate the effective implementation of the Federal Source Code Policy. This platform enables agencies to identify whether their software needs can be satisfied via an existing Federal Government solution prior to procuring new software, thereby cutting wasteful spending and avoiding duplicative acquisitions. When the platform was launched in 2016, it represented 45 software projects. Today, the platform represents over 3,000 projects across the federal government.

Growth and engagement across Code.gov has been steadily increasing throughout FY17. Many projects that are represented on the platform have been reused several times, enabling agencies to realize substantial time and cost savings by avoiding duplicative software development. For example, analytics.usa.gov – a website built by GSA that tracks real-time traffic to government websites – has seen reuse not only by other federal agencies, but also by several city and state governments. Code.gov continues to engage with federal agencies to facilitate effective code sharing and collaboration across the government. By emphasizing code reuse, the government will continue fulfilling its objective to cut wasteful spending, save taxpayer dollars, and improve the fidelity of government source code across the country.

SECTION II: GOVERNMENTWIDE IT WORKFORCE AND TRAINING POLICIES

Section 209 of the E-Gov Act (44 U.S.C. § 3501 note) requires OPM, in coordination with OMB, the Chief Information Officers (CIO) Council, and GSA to analyze the personnel needs of the Federal Government related to IT and information resource management. The E-Gov Act further states that this group must identify where current training does not satisfy current personnel needs, and that it must issue policies to promote development of performance standards for training. In accordance with Section 209 of the E-Gov Act, this section provides a summary of FY 2017 activities related to IT workforce policies, evaluation, training, and competency assessments. Appendix H of this report provides examples of agency-specific training initiatives.

OPM continues to be actively engaged in Government-wide cybersecurity work. In 2015, Congress passed the Cybersecurity Workforce Assessment Act, which focused on improving cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats and other purposes. It covered four components, including the development of a Federal Cybersecurity Workforce Assessment, which included, among other things, common definitions, a national cybersecurity workforce measurement initiative, identification of cyber-related roles of critical need through the NICE framework, and Government Accountability Office (GAO) status reports.

In February 2016, the Cybersecurity National Action Plan (CNAP) was published, which identified near-term actions and puts in place a long-term strategy to enhance cybersecurity awareness and protections, protect privacy, maintain public safety as well as economic and national security, and empower Americans to take better control of their digital security. In July 2016, OPM and OMB issued the Federal Cybersecurity Workforce Strategy. This strategy, as required by CNAP, was the result of hundreds of federal and private sector inputs. OPM, in partnership with OMB, has achieved the following implementation goals since the release of the Federal Cybersecurity Workforce Strategy:

- Goal 1: Workforce Needs/Workforce Planning
  OPM is leading the Government-wide adoption of a new coding structure aligned to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework and will continue to actively provide guidance, training, and technical assistance to all agencies. By April 2018, agencies will complete coding all cybersecurity positions under the NICE Framework as required by the Federal Cybersecurity Assessment Act of 2015.

- Goal 2: Expand the Federal Pipeline through Education and Training
  OPM briefed students from 146 (68% of the total 214) Centers of Academic Excellence, as well as 60 of the 69 Scholarships for Service schools, and students from 116 other colleges and universities with cybersecurity programs. Briefings included: "Pathways Programs for Students and Recent Graduates," "Finding and Applying for Federal Jobs/Navigating USAJOBS," and "Writing Your Federal Resume."

- Goal 3: Recruit and Hire Highly-Skilled Talent
  OPM established a Government-wide Cybersecurity Human Resources (HR) Cadre comprised of representatives from each Chief Financial Officer (CFO) Act agencies to improve HR delivery to Chief Information Officers (CIOs). OPM released a Strategic Recruitment for Cybersecurity Model on July 25, 2017, which provides guidance to agencies on how to secure top cybersecurity talent through building talent pipelines, cultivating and maintaining partnerships, monitoring recruitment activities, and sharing accountability. OPM issued Direct Hire authority for Information Technology (Information Security) GS-2210 positions and is exploring Direct Hire for additional Qualifying Cybersecurity Occupations.

- Goal 4: Retain and Develop Highly Skilled Talent
  On July 12, 2017, OPM hosted the 2nd Government-wide Cybersecurity Orientation with over 200 participants. OPM also drafted legislation on Cybersecurity Skills and Education Incentives to obtain and retain credentials. Cybercareers.gov was launched as a Government portal aimed to support a "one stop shop" for Hiring Mangers and Job Seekers. The site is being further tailored to for students and universities, as well as current Federal employees. OPM expanded the Presidential Management Council (PMC) Rotation program to include a dedicated participant from each agency's CIO community. OPM coordinated a cybersecurity training for non-cyber professionals to increase foundational cybersecurity knowledge to career fields outside of the cyber workforce. The training, Federal Executive Cybersecurity Seminar, was offered September 12, 2017 at Department of Homeland Security.

In May 2017, the President signed Executive Order (EO) 13800: *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. The E.O. sets forth policy for management of cybersecurity risk executive-branch-wide and requires agency heads to lead integrated teams of senior executives with expertise in IT, security, budgeting, acquisition, law, privacy, and human resources. Specifically, the E.O. requires the Department of Commerce (DOC), the Department of Homeland Security (DHS), the Department of Defense (DOD), the Department of Labor (DOL), and OPM to assess the scope and adequacy of efforts to educate and train the American cybersecurity workforce of the future. These agency partners have drafted the IT Modernization Report to the President summarizing their findings and providing in-depth recommendations aimed at supporting the growth of the Nation's public and private sector cybersecurity workforce.

SECTION III: DISASTER PREPAREDNESS

Consistent with Section 214 of the E-Gov Act (44 U.S.C. § 3501 note), this section was developed in consultation with DHS and the Federal Emergency Management Agency (FEMA) to provide a summary of activities that maximize the use of IT for disaster management, including use of IT to enhance and support crisis preparedness and response.

The Disaster Assistance Improvement Program

The Disaster Assistance Improvement Program (DAIP) maintains a Government-wide, single portal for disaster survivors to submit electronic applications for assistance. DAIP's mission is to ease the burden on disaster survivors by providing them with a mechanism to request and access disaster assistance through the collaborative efforts of Federal, state, local, tribal, and nonprofit partners.

Following a presidentially declared disaster for individual assistance, survivors in need of assistance can register online at DAIP's DisasterAssistance.gov. The *DisasterAssistance.gov* portal provides disaster survivors with a single source for potential assistance programs, easy access to the application, application updates, and disaster-related information. The secure portal ensures that disaster survivors, who may be displaced or otherwise out of contact, have access all Federal agencies that offer forms of disaster assistance, and continue to receive benefits from non-disaster related assistance programs.

In FY 2017, DAIP provided Registration Intake (RI) for 54 presidentially declared Individual Assistance (IA) disasters. It hosted 33,182,231 *DisasterAssistance.gov* site visits. It also registered 3,125,579 registrations for disaster assistance via call center support and internet transactions (1,676,127 using Desktops, 1,180,486 using Mobile Devices, 268,966 using FEMA Call Centers). The program continues to receive high customer satisfaction scores from survivors using the site. The program achieved "green" ratings from the DHS Office of Accessible Systems and Technology and the DHS Office of the Chief Information Officer Program Health Assessment.

OpenFEMA is the vehicle used to share high level DAIP metrics. Through OpenFEMA, Housing Assistance and Registration information statistics are shared at the zip code level along with over 30 other datasets. This information provides a detailed recovery snapshot to Government, non-profits and other community partners. Overall, the OpenFEMA API received approximately 2 million hits per week and continues to be a central source for public FEMA data.

SECTION IV: GEOSPATIAL

In accordance with Section 216 of the E-Gov Act (44 U.S.C. § 3501 note) this section provides a summary of activities related to the development, acquisition, maintenance, distribution, and application of geographic information. This includes common protocols that improve the compatibility and accessibility of unclassified geographic information and promote the development of interoperable information systems technologies that allow widespread, low-cost use, and sharing of geographic data by Federal agencies, state, local, and tribal Governments, and the public.

The Department of the Interior (DOI), as the managing partner, plays an important role in helping to facilitate the Government's efforts for the Geospatial Platform Shared Services initiative, which is led by the Executive Secretariat for the Federal Geographic Data Committee. In its third full year of development and operations under a technical development team, DOI made important improvements to enhance the National Geospatial Platform (GeoPlatform.gov, also known as GeoPlatform). DOI greatly improved productivity, integration, interoperability, lifecycle management, availability, utility, robustness, reliability, efficiency, and mission effectiveness. Improvements focused on geospatial data and service search, discovery, access, and use across the GeoPlatform's well-integrated, yet diverse ecosystem of Federal geospatial assets. In keeping with the NSDI and Open Data visions, these efforts greatly lowered the barrier for government, public, and commercial users to share and exploit national data and service assets through a common, harmonized framework. The GeoPlatform also made substantial progress advancing digital community experiences, improving the means for Federal agencies and partners to better collaborate on national challenges, while enhancing productivity in building new communities, and enhancing end-user functional and content experiences.

In 2017, the *GeoPlatform.gov* also served as a collaboration and information delivery resource for DOI, DHS, and the National Geospatial Agency during critical response efforts for national disasters. In response to Hurricane Harvey, Irma, and Maria, Homeland Infrastructure Foundation-Level Data (HIFLD) inter-agency members developed a common centralized open site on the GeoPlatform to host and publish unclassified publicly available geospatial data. Both HIFLD4Harvey and HIFLD4Irma, which were also used to support Hurricane Maria, registered over 12,850 users with over 2,920 downloads in a little over 30 days. This first-of-its-kind operational response was received with great enthusiasm and garnered direct positive feedback from Federal agencies and on-the-ground first responders.

FEMA and the Civil Air Patrol (CAP) also used the GeoPlatform shared service to launch a new CAP image browser. The tool allows aircrews to identify the aerial image collection for the day and to focus on particular areas in Puerto Rico and the neighboring U.S. Virgin Islands. This new tool will help expedite the aerial damage assessment process for aircrews, ensuring that each photo taken is processed, tabulated, and tagged as quickly as possible and ready for a timely review by FEMA, the US Air Force, and other Government entities involved in the response to Hurricane Maria. CAP aircrews flew over 131 sorties and provided more than 36,000 images in support of the response to Hurricane Maria.

Additionally, the GeoPlatform continued to evolve in the DOI cloud environment, as a cohesive national geospatial system-of-systems that provides a seamless, secure gateway to national geospatial assets. The GeoPlatform continued to improve the ability for stakeholders to manage their diverse portfolios through enhanced data, metadata, and service lifecycle management. This improvement in the platform and its toolsets supported improved transparency, cost avoidance, and Open Data sharing. In addition, these platform enhancements support the implementation of OMB Circular A–16, "Supplemental Guidance," which directs Federal agencies to manage their National Geospatial Digital Archive (NGDA) as a single portfolio for use across Federal agencies, their partners and the public, while making it available through the GeoPlatform.

CONCLUSION

In 2002, Congress passed the E-Gov Act in response to the growing use of computers and the internet by the public, rapidly transforming societal interactions and the relationships between citizens, private business, and all levels of Government. In an effort to provide effective leadership and streamline Federal initiatives, OMB was tasked to spearhead efforts to develop and promote electronic Government services across the Federal Government. One of the key initiatives of this legislation was to improve the ability of the Government to achieve agency missions and program performance goals by promoting the use of emerging technologies across the Federal agencies to provide citizen-centric services and increase public access to Government information and data. Building on the objectives of this legislation, the OFCIO within OMB has undertaken three broad goals for IT in the Federal Government: (1) to reduce waste and duplication, and ensure that IT investments stay within their budgets and deliver on time; (2) to help agencies deliver IT investments that maximize the Government's productivity and customer satisfaction; and (3) to expand the use of data and analytics to support agency IT portfolio management.

Since the passage of the E-Gov Act, Federal agencies have made significant progress in using emerging technologies to enhance citizen-facing services and grow citizens' access to Government information. This report highlights many of these innovative activities that will improve Government efficiency and delivery of services to the public, as required by the E-Gov Act.

APPENDICES: COMPLIANCE WITH OTHER GOALS AND PROVISIONS OF THE E-GOV ACT

This section provides a description of highlights of Federal agency compliance with other goals and provisions of the E-Gov Act. The subsections below are listed in order according to the corresponding sections of the E-Gov Act. The information contains broad overviews of what agencies are doing to comply with the goals of the E-Gov Act, and also includes some agency-specific illustrations of approaches to complying with the provisions of the Act. To view additional agency descriptions of compliance with provisions of the E-Gov Act, please visit the IT Dashboard E-Gov Act Reports Page.

As part of the broader OMB effort to eliminate duplicative data collections and reduce reporting burden placed on Federal agencies, OMB did not request information for several appendices in its annual E-Gov Act implementation data collection this year. Specifically, information was not collected from agencies that in past reports would have been included in Appendix D, Appendix E, Appendix F, and Appendix G. Please read explanations in each of these sections noting primary sources where this information can be found.

Furthermore, several of the requirements set forth in the E-Gov Act require the provision of web addresses to specific content on agency websites. Due to the nature of these requirements, summaries of the following submissions are not included in the appendices but are included on the IT Dashboard:

- Accessibility: In accordance with Section 202(d) of the E-Gov Act, this section provides URLs for agency websites describing the actions taken by agencies in accordance with section 508 of the Rehabilitation Act of 1973, as amended by the Workforce Investment Act of 1998, Pub. L. No. 105-220.

- Internet-Based Government Services: In accordance with Section 204 of the E-Gov Act, www.USA.gov serves as an integrated internet-based system for providing the public with access to Government information and services. In accordance with Section 207(f)(3), this section provides URLs for agency activities on *www.USA.gov*.

- Freedom of Information Act: In accordance with Section 207(f)(1)(A)(ii) of the E-Gov Act, this section provides the URLs for agencies' FOIA websites.

- Information Resources Management Strategic Plan: In accordance with Section 207(f)(1)(A)(iv) of the E-Gov Act, this section provides the URLs for agencies' Information Resources Management strategic plans.

- Public Access to Electronic Information: In accordance with Section 207(f)(1)(B) of the E-Gov Act, this section provides URLs that contain agency customer service goals and describe activities that assist public users in providing improved access to agency websites and information, aid in the speed of retrieval and relevance of search results, and use of innovative technologies to improve customer service at lower costs.

- Research and Development (R&D): In accordance with Section 207(g) of the E-Gov Act, this section provides URLs for publicly accessible information related to R&D activities and/the results of Federal research.

APPENDIX A: ENHANCED DELIVERY OF INFORMATION AND SERVICES TO THE PUBLIC

The E-Gov Act requires OMB to oversee the implementation of a number of programs relating to capital planning and investment control for information technology; the development of enterprise architectures; information security; privacy; access to, dissemination of, and preservation of Government information; accessibility of information technology for persons with disabilities; and other areas of electronic Government.[4] The Act requires OMB to sponsor ongoing dialogue to encourage collaboration and enhance understanding of best practices and innovative approaches in acquiring, managing, and using information resources to improve the delivery of Government information and services to the public.[5] This appendix describes agency activities that enhance delivery of information and services to the public, improve or enable more data-driven decision-making in Government operations, and enhance interoperability between different public and private sector entities. The full list of activities can be found on the IT Dashboard.

Agencies are undertaking numerous initiatives to provide the public with increased transparency and availability to Government data. In May 2017 the Treasury Department in collaboration with OMB, released an innovative new public display of Federal financial information on Beta.USAspending.gov. A crucial element of the new website is a standardization of key data elements promoting transparency and enabling the agencies, Congress, and taxpayers to track spending from appropriations all the way to final recipient. OMB and partner agencies continue to seek feedback from key stakeholders driving continuous iterations and improvement to ensure a transparent and open government approach. The "beta" site will continue to run concurrently with the previous version of *USAspending.gov* to minimize disruptions to users' data access and provide more time to add user-centered enhancements until the beta site is production ready.

Similarly, NASA made improvements to its Open NASA.gov platform, which serves as a gateway to NASA's Open Government activities, providing interactivity for users inside and outside NASA who want to engage with NASA's data, code, application program interfaces (APIs) and tools. At the heart of the site is the main NASA data registry that allows users to search metadata records of NASA data that exist on NASA authoritative sources, view and interact with hosted data through APIs, gain insight and developer details on NASA API's, and collaborate and create visualizations with NASA data. In addition, the site allows users to maintain profiles, which enable the creation of data communities. The newly created Research Access page provides citizens and researchers access to NASA's Data Management Plan with instructions for NASA-funded researchers receiving grants, cooperative agreements, and contracts for research.

At the Department of Education (ED), the InformED platform was established to increase the availability of ED's public data, ensuring universal access, and catalyzing the data's reuse. In

[4] See 44 U.S.C. § 3602(e).
[5] See 44 U.S.C. § 3602(f)(9).

FY 2017, InformED invested in new technologies and approaches that simplified access to information and empowered citizen innovators, including acquiring autoAPI, an open source CSV-to-API engine used to create several APIs on top of the Civil Rights Data Collection. In addition, InformED awarded a contract for an open data investment feasibility study, which has brought in critical expertise to assess the agency's barriers to open data. InformED also developed and applied a mobile-friendly data story template that strengthens the Department's ability to deliver rich and accessible data narratives. Every new data story expands a code base that ED can return to repeatedly to build effective data visualizations. Finally, ED launched its first developer hub and an official account on GitHub to increase engagement with developers.

The Department of Health and Human Services (HHS) continued to utilize HealthData.gov to make appropriate datasets available to the public to fuel solutions in health and human services. After remodeling the website in FY 2016, stronger administrative services are in place for data curators, as well as an enhanced facilitation data cataloging and management process that builds catalog integrity and supports better metadata management. In FY 2017, the HHS Office of the Chief Information Officer (CTO) is creating a comprehensive dataset of HHS, state, private, and Federal data in reference to the opioid epidemic.

Similarly, in FY 2017 the National Archives and Records Administration (NARA) implemented enhancements to the National Archives Catalog API to improve the delivery of Catalog data to the public, making access to the large volumes of data in the Catalog more efficient for the user. In addition, these enhancements improved the ability of NARA staff to develop a more robust web search engine and web pages using Catalog data, which will become a more effective presentation of Catalog data. The enhancements include deep paging, exact search, with/without field value search, and including comment IDs in the data.

The US Agency for International Development (USAID) in FY 2017 continued to expand the breadth of data it makes available to the public via its Development Data Library (DDL). For example, in April of 2017, USAID Colombia hosted a data jam to challenge participants to analyze data sets and devise solutions to problems affecting rural development in the country. Participants used advanced statistical and machine learning methods to create new approaches to increase supply chain productivity, generate employment, and encourage youth participation in rural economies. In August of 2017 the International Food Policy Research Institute (IFPRI), an USAID partner, hosted a data-thon showcasing findings from the Feed the Future Initiative based on data generated in Bangladesh. The data spanned four key food security-relevant domains (climate, agriculture, nutrition, and gender) which enabled analysts and visualization specialists to generate new insights related to climate shocks and female empowerment in the agricultural sector.

Agencies are furthermore addressing public needs through targeted services, like those that connect recipients and providers of services. For example, the DHS Digital Service team partnered with the US Customs and Border Protection (CBP) to launch a new online application for Global Entry, and other CBP Trusted Traveler programs. The new system, with a focus on usability, created a simpler interface for users to quickly join and renew their Trusted Traveler membership, integrating Login.gov to provide a secure, two-factor login and authentication process. This was also the first major application CBP has moved to the cloud, and it is serving

as the template for future cloud adoption. The new application launched on October 1st, 2017 after about nine months of development – half the amount of time originally projected—and has already had over 500,000 accounts created.

Another initiative is DOI's Recreation One Stop (R1S) which is an interagency partnership that provides reservation services, sharable data, and recreation trip-planning tools for people who wish to visit federal lands and waters across the United States. Currently, Recreation.gov provides information regarding more than 3,400 individual facilities, with more than 90,000 campsites, 46 ticketed tours or events, and 54 high-demand locations accessed by permit or lottery. In 2017, there were more than 37 million sessions, 19 million visitors, and 344 million page views to *Recreation.gov*, which represents a 26 percent increase in visitation to the website, compared to 2016.

Working with industry partners, the Department of Transportation (DOT) and the Federal Aviation Administration (FAA) created a simple online tool that enables operators to register their Unmanned Aircraft Systems (UAS). As of October of 2017, 923,443 people have registered online to fly. In addition, the FAA is currently developing the "FAA DroneZone" to make a "one-stop-shop" for all things UAS in the FAA – registration, accident reporting, waiver and authorization requests, training, and special alerts or notifications. Currently the FAA is developing the modules and expects the DroneZone be available to the public by March of 2018.

The Department of State's (State) ForeignAssistance.gov (FA.gov) application enhances the delivery of information and services to the public. *ForeignAssistance.gov* specifically tracks U.S. Government assistance provided to more than 100 countries around the world. In addition to raising public awareness for U.S. foreign assistance around the world, *FA.gov* will help recipient governments manage aid and inform budgeting and planning decisions, empower citizens to hold their governments accountable for the aid they receive, and support data-driven development. The site currently contains data on planning, obligations, and disbursements on a transactional level, with performance data and descriptive narrative data also available for State and USAID. In addition, *FA.gov* recently launched the "Analyze" feature, a custom data visualization tool that enables users to overlay foreign assistance data with other open data and development indicators to investigate trends over time or across countries, regions, and income groups. Soon all 22 agencies with foreign assistance funding in their portfolio will be reporting to *FA.gov*.

The Social Security Administration (SSA) has made significant improvements to its "my Social Security" program, an online portal that provides the public the ability to access personalized services and perform online transactions via a secure account. Originally launched in 2012, the site was expanded in 2015 to include non-beneficiary services and to include the ability to request a replacement SSN card and retrieve a machine-readable version of the Social Security Statement. As of October 2017, over 32.4 million customers have registered for a mySocialSecurity account. In FY 2017, customers conducted over 155 million online transactions. In addition, the internet Social Security Number Replacement Card (iSSNRC) application became available in 10 new states in FY 2017 including California, Texas, and Florida. Over 600,000 cards have been issued via iSSNRC, with the application now available in

24 states and Washington, DC. SSA plans in 2018 to further enhance its new wage reporting tool (myWageReport) and expand access to SSI recipients.

Government-wide, agencies are also diversifying their information resource capabilities, with some providing data in both navigator formats and in Application Program Interfaces (APIs), and working to improve the usability of data and websites by leveraging public feedback mechanisms. For example, the Department of Justice (DOJ) is improving the user experience of FOIA.gov through the introduction of augmented and enhanced functionality aimed at public users and federal agencies. With an average of over 730,000 FOIA requests submitted annually over the last four years, it is essential that the system for collecting requests be user friendly and the underlying processes efficient. The new iteration of *FOIA.gov* will assist public users in identifying agencies of interest through a series of controlled questions, as well as, allow the user to submit a structured FOIA request without navigating to another site or launching an email application. As a part of this effort, DOJ solicited public input and research, as well as, collaborated with multiple federal agencies in order to deliver functionality with the greatest benefit to all. DOJ is planning to launch this new functionality for public use in early 2018 with additional features further improving the user experience provided in the future.

In FY 2017, the USA.gov platform connected people more than 200 million times with Government information through its websites, social media, publications, email, and phone calls through the USA.gov Contact Center. Managed by GSA, the site has the goal to make it easier for the public to find and consume U.S. Government information and services on the web. USA.gov makes content accessible to the broadest audience possible, and recently implemented a responsive design approach on its websites to ensure consistent user experience on any device, leading to 25 percent growth in both mobile and tablet usage. The landing page and navigation features of USA.gov were also redesigned to improve user engagement. Additionally, USA.gov integrated BusinessUSA content and developed a unique faceted search tool to help small businesses find business opportunities and grants.

In FY 2017, OPM worked to transform USAJOBS from a job board to a Federal career portal through the implementation of seven production releases. A number of enhancements were made to the site, including: (1) enhancement of the collection of demographics collected at the time of application, (2) redesign of the Agency Talent Portal resume mining feature, (3) upgrades to the search architecture, (4) implementation of a new search user interface that introduced hiring paths to address eligibility, as well as, assisted authoring to address keyword nomenclature issues, (5) redesign of the job announcement (6) implementation of campaigns and events in the Agency Talent Portal and (7) development of new structural changes to the Staffing Integration Framework to improve job announcement fields that are submitted by Talent Acquisition System providers to display on *USAJOBS*. The program office conducted extensive user research and usability testing throughout the design and implementation phases to ensure the products meet user needs. Lastly, the program acquired a new product, Open Opportunities, a platform originally built by GSA to provide an opportunity board for short-term, micro-detail tasks. This product will expand *USAJOBS'* offering for the federal workforce to find and apply to developmental opportunities.

APPENDIX B: PERFORMANCE INTEGRATION

In accordance with Section 202(b) of the E-Gov Act (44 U.S.C. § 3501 note), this appendix describes what performance metrics are used and tracked for IT investments, and how these metrics support agency strategic goals and statutory mandates. Agencies provide a variety of performance metrics, including those that focus on cost and schedule of projects, risk factors, customer service, and innovative technology adoption and best practices. Select efforts are described in further detail below. The full list of activities and many of the aforementioned OMB metrics can be found on the IT Dashboard.

Performance metrics are an essential tool for determining the health, risks, and future needs of agencies' IT projects, These metrics are a product of both the project teams and agency CIOs designing and tracking performance metrics that support the strategic goals and statutory mandates of the agency. To strengthen links to departmental priorities, major IT investments are mapped to specific elements of the agencies' strategic plans and performance measures are required elements of each Business Case. Particular focus is paid to FITARA implementation requirements, as outline in OMB memorandum M-15-14: *Management and Oversight of Federal Information Technology*. OMB is responsible for ensuring FITARA's many IT governance, transparency, and risk-management provisions are successfully implemented by agencies. One useful tool OMB utilizes is the FITARA Scorecard, which assigns 24 agencies grades from A to F in several implementation categories. The Government Accountability Office (GAO) and House Oversight and Government Reform Committee issue scorecards twice a year, with grades released in June and November for 2017. The November 2017 scorecard saw three agencies increase their overall scores from the June 2017 report (ED, OPM, SBA), with six agencies receiving a decrease in rating, and fifteen agencies with no change.

Agencies continue to develop and utilize IT governance and management processes, ensuring that senior agency officials, including the agency CIO, play an active role in reviewing performance metrics for agency IT portfolios. For example DOC has its own Commerce IT Review Board (CITRB), which periodically evaluate agency IT investments during its program/project lifecycle. The CITRB is co-chaired by DOC's CIO and CFO, and holistically evaluates IT Project/Program and Portfolio performance, progress risk and health. Finally, ED uses a similar department entity, the Planning and Investment Review Working Group (PIRWG) to select, control and evaluate the IT investments that go into the Department's IT portfolio.

Effective IT governance involves a holistic approach, where the agency updates its strategic plans (such as IRM & TBM strategic plans) focusing on deliverable defined in its business cases and programs, outcome metrics and an effective governance process with the right level of executives with authority to come to the table. Many agencies have created their own multi-year strategic plans for management of their IT portfolios. For example, DOJ performance goals for enterprise IT are set forth in the DOJ Strategic Plan for Information Services and Technology 2015-2018. This plan defines key goals, strategies and objectives for the department's IT organization. DOJ is in the process of updating its Strategic Plan for Information Services and Technology early in FY 2018, identifying goals and objectives for the 2018-2020 timeframe. Likewise, Treasury in FY 2017 refined its own investment risk rating process and

algorithm to apply more rigors in its review of the IT investment portfolio toward agency objectives, strategic goals, and statutory mandates to complement existing operations and performance metrics.

In a similar effort, the Small Business Administration (SBA) took steps to link performance goals to key stakeholders, private sector, Federal agencies, and international operations through strategic goals and objectives. The SBA 2014-2018 Strategic Plan, includes IT investment management in its strategic objective 3.1 (Program Operations). The SBA tracks IT performance through a customer satisfaction survey and security incidents reported through US CERT (United States Computer Emergency Readiness Team). As the SBA develops its FY 2018-2022 Strategic Plan, a strategic objective for information technology has been established with a new performance goal that tracks IT costs savings. Finally, Department of State (DOS) has its own IT Strategic Plan for FY 2017 – 2019, which defines goals, objectives, and performance measures for enterprise IT in support of the State's missions and strategies, and will be updated based on specific recommendations and objectives from the Department of State's Redesign Initiative.

Many Federal agencies have used these performance metrics and oversight activities to identify initiatives ripe for improvement and modernization. For example, the Federal Motor Carrier Safety Administration (FMCSA) within DOT implemented the first two phases of a multi-year program to modernize the registration process for commercial motor vehicles. This initiative provides a new streamlined online system that simplified the FMCSA registration process. Phase I helped clean more than 360,000 inactive carriers from the registration system. This effort also saves time, money, and lives by allowing inspectors to focus on the most dangerous carriers. An estimated 11,500 hours of annual investigation time will be saved each year, resulting in 547 additional investigations that can be performed; potentially preventing up to 65 crashes, 40 injuries, and saving 2 lives. Phase II launched a single, online application system for all new applicants, replacing multiple forms. New applicants only include those never assigned a USDOT or MC number. This effort saves applicants and industry service providers over one hour per application, with cost savings of $1.6M realized in just the first 6 months. In addition, this new online application system, utilizing the Utility for Risk Based Screening and Assessment (URSA) tool, facilitates vetting operations by automatically screening applications for carriers attempting to become a "reincarnated" version of a previous or existing high-risk operator. The URSA tool, to date, has screened over 75,000 new applications for operating authority, flagged over 7,000 of them for further investigation, resulting in 175 carriers being rejected due to high risk behavior. These rejections are projected to prevent 12 crashes and save 4 lives per year. The final phase will combine multiple registration processes, consolidate information technology systems, and consolidate as many as 15 forms into a single registration online platform.

OMB IT Efforts on Performance Integration--TBM

Since the passage of the Clinger-Cohen Act in 1996, OMB has been tasked with conducting oversight around Agency IT spending and ensuring the effective application of Congressional funding for IT. Each year, OMB requires agencies to manually report IT budget formulation and execution data to be captured, analyzed, and displayed to the public on the IT

Dashboard. In addition, agencies provide performance, risk, and project management data for each major IT Investment in their respective portfolios to be displayed as well. To address persisting data quality concerns and achieve burden reduction for agency reporting, OMB is actively collaborating with agencies to leverage all available authoritative data and implement automation wherever possible.

Agencies develop unique performance measures for each project in their respective IT portfolios, focusing on mission and business results, customer service, and improvements to business processes and technical goals for operational IT systems. Every major IT investment must contain results-specific metrics to measure their effectiveness in delivering the desired service or support level required to enable successful mission outcomes. OMB's Capital Planning and Investment Control (CPIC) establishes the processes and tools for selecting, controlling, and evaluating IT projects that comprise the IT portfolio.

In FY 2017, OMB began implementation of a long-term strategic paradigm shift and made a significant update to the annual CPIC reporting process for FY 2019 agency budget submissions through introducing the Technology Business Management (TBM) Framework to categorize IT spending. Leveraging a taxonomy that is proactively managed by a non-profit organization alleviates some of the need for the Federal Government to identify, define, and achieve consensus on the standards and terms used to report IT costs, thereby ensuring the viability and long-term sustainability of this system. In the future, Federal IT budget data aligned with the taxonomy will become the basis for the IT CPIC process and OMB oversight of agency's IT portfolios.

As OMB continues its implementation plan through the FY 2020 guidance, it is partnering with Agencies to promote maturation in reporting processes and data quality while introducing the last remaining Part 3 Infrastructure Standard Investment Reports. Simultaneously, OMB is introducing a new Standard Investment Report for Part 2 Support Services Standard Investment Reports to support the gradual implementation of the TBM taxonomy's Services layer. Long-term implementation remains on schedule to complete the CPIC transition to TBM reporting by the FY 2021 reporting cycle.

Aligning Federal IT management with TBM industry standards will allow more effective management and oversight of agency IT investments. Full implementation of the TBM taxonomy will enable the Federal Government to 1) benchmark its IT performance and cost data against industry to more effectively identify and leverage best practices; 2) locate instances of over or under-funding for IT services and infrastructure to more efficiently allocate funding across Agencies; and 3) enable Government decision-makers to tie Agency mission priorities to specific IT funding decisions by providing unprecedented transparency into their organizations' spending on technology and innovation. This granularity will help gradually align the categorization of costs with policies around IT modernization, CIO authorities, commodity IT management, category management, and data center optimization, among others.

APPENDIX C. GOVERNMENT-PUBLIC COLLABORATION

In accordance with Section 202(e) of the E-Gov Act (44 U.S.C. § 3501 note), this appendix describes how agencies utilize technology to initiate Government-public collaboration in the development and implementation of policies and programs. They do so through a variety of approaches, including using public meetings on agency websites, engaging with the public through website comments and email lists, and using online portals to facilitate public participation in regular agency processes. Select efforts are described in further detail below. The full list of activities can be found on the IT Dashboard.

Federal agencies continue to leverage technology to initiate Government-public collaboration in the development and implementation of policies and programs. For instance, the DOD used the Federal eRulemaking portal (discussed more in Appendix E) to facilitate public participation in its regulatory process. During FY 2017, DOD used this portal to elicit comments from the public on which of its existing regulations should be considered for repeal, replacement, or modification. The identification and elimination of unnecessary, outdated, or ineffective regulations will alleviate unnecessary burden on the public and ensure the Department continues to meet its fiduciary responsibilities to the American people.

In a similar effort, DHS sought to solicit input and foster an online conversation revolving around the 2018 Quadrennial Homeland Security Review (QHSR). To accomplish this, DHS utilized Ideascale, a crowd-sourcing collaboration platform. During FY 2017, DHS posted topics related to its strategic development work, moderated and contributed to discussions, and incorporated key ideas into its strategy review process, as appropriate. Some of the many topics that were posted and discussed on Ideascale include border and aviation security, terrorism, immigration, and cyber security. DHS will present their Quadrennial Homeland Security Review to Congress at the end of 2017 as required by law.

In FY 2017 NARA also sought input from the public on its draft 2018-2022 Strategic Plan, making the draft available to the public on GitHub. NARA sought feedback through posting issues on GitHub or sending comments by email. By publishing the Draft Strategic Plan on GitHub, NARA offered a transparent way for stakeholders to comment and to view revisions. The open source approach also makes it easy for other organizations to reuse the framework for their own plans. The code and all contributions to this project will be released in the public domain under the CC0 dedication. A revised plan was published on September 15.

Finally, DOJ also sought public comments on regulatory matters. In February 2017, the President issued Executive Order 13771: *Enforcing the Regulatory Reform Agenda*, which set forth principles and requirements for each agency to evaluate and implement measures to lessen the regulatory burden on the American people. In response, the DOJ established a Regulatory Reform Task Force that sought public comments on the various kinds of actions taken by DOJ components that the public perceives to be regulatory in nature. The DOJ Regulatory Reform Task Force is considering these public comments as it conducts its own evaluation of the Department's regulations, in order to identify candidate regulations for repeal, replacement, or modification.

Many agencies also developed online hubs to better provide information to the public and foster public engagement on various agency initiatives. For example, in FY 2017 Benefits.gov, managed by DOL, received almost 9.4 million site visits and reached a record of more than 1.2 million site visits in August. *Benefits.gov* is the official benefits website of the U.S. Government, providing citizens with information and eligibility pre-screening services for more than 1,200 Federal and State benefit programs across 17 Federal agencies. In addition, *Benefits.gov* completed the procurement of Microsoft Azure in FY 2017, a commercial cloud-hosting provider which will better position *Benefits.gov* to shift to emerging technologies in the future. To mark the 15th anniversary of the site, there was an increased focus on customer engagement and outreach, resulting in 3,100 new followers on its Facebook and Twitter pages, a 191% increase in referral traffic to the benefits.gov website, and a 48% increase in Compass eNewsletter subscribers.

In addition, State also rebranded its Virtual Student Foreign Service program to the Virtual Student Federal Service (VSFS) program to recognize the advancement of the program as it now supports over 30 Federal agencies. The VSFS is supported by an innovative, cloud-based information technology application that facilitates all aspects of the initiative, including project submission by agencies, as well as the student application and selection processes. The program had a record year in FY 2017 with more than 4,600 U.S. college undergraduate and graduate students applying for 1,300 position available this cycle to work on 525 projects for various Federal agencies.

Similarly, in March 2017 the Nuclear Regulatory Commission's (NRC) Office of Administration deployed a centralized rulemaking tracking and reporting tool. The web-based system provides internal and external stakeholders with consistent, accurate, and up-to-date information on all of the agency's planned rulemaking and petition for rulemaking (PRM) activities. The information from this system is available to the public on NRC's public website, under the "Public Meetings & Involvement" tab.

Finally, the Intelligence Advanced Research Projects Activity (IARPA), an office within the Office of the Director of National Intelligence (ODNI), continued to utilize the Federal Business Opportunities (FBO) portal as its primary vehicle to initiate collaboration with the public for research. During FY 2017, IARPA posted more than 24 announcements on FBO for new program Broad Agency Announcements (BAA) and Requests for Information (RFI). More than 230 abstracts and proposals were received from industry and academia in response to the announcements, and more than 500 people attended the resulting 8 public collaboration events IARPA hosted.

One final way many agencies worked to increased Government-public collaboration was by funding research projects. For example, in FY 2017 USAID's U.S. Global Development Lab announced $10 million for 49 new research projects to address evidence gaps and advance technical capacity in critical areas of development. The 49 new projects span 23 USAID partner countries and are funded through the Partnerships for Enhanced Engagement in Research (PEER) program, an initiative designed to foster collaborative global research. These new

awards will allow Government-public collaboration on a variety of crucial research areas, such as wildlife protection, biodiversity conservation, water resource sustainability, satellite monitoring of natural resources, fisheries management, food security, disaster mitigation, and others.

APPENDIX D. CREDENTIALING

Section 203 of the E-Gov Act (44 U.S.C. § 3501 note) requires the Federal Government to describe current activities agencies are undertaking to achieve the interoperable implementation of electronic credential authentication for transactions with the Federal Government.

An important part of the Federal Government's information security standards is Identity, Credential, and Access Management (ICAM). The goal of ICAM is to implement a set of capabilities that ensure network users use strong authentication to access Federal IT resources and to limit users' access to the resources and data required for their job functions. Mature ICAM programs enable agencies to monitor users' access and implement secure capabilities such as single sign-on, which provide trusted users with efficient access to applications and data.

The Federal Government has sought to implement these security standards through the issuance of Personal Identity Verification (PIV) cards. The establishment of the PIV credential as part of a broader enterprise solution enables common service capabilities in secure and reliable transactions. The ICAM goal consists of PIV enforcement targets for privileged users (100%) and unprivileged users (85%). Many Federal agencies have made significant progress in implementing and adopting the use of PIV cards, with agency implementation progress collected and monitored as part of the annual Federal Information Security Management Act (FISMA) metrics. For FY17, civilian CFO Act agencies reported 87% for unprivileged users (up from 81% reported in FY16) and 98% for privilege users (up from 89% reported in FY16).

As part of the broader OMB effort to reduce reporting burden places on Federal agencies, OMB did not request this information in its annual E-Gov Act implementation data collection this year. For information on agency initiatives in implementing security standards, including the adoption of PIV cards, please see OMB's FY17 FISMA Report.

Commented [MZTE(4]: Link once the FY17 report is released.

APPENDIX E. E-RULEMAKING

One of the goals of the E-Gov Act (44 U.S.C. § 3501 note) is to assist the public, including the regulatory community, in obtaining access and electronically submitting comments on rulemakings by Federal agencies. Specifically, Section 206 of the E-Gov Act lays out requirements designed to not only increase engagement with the public, but to increase collaboration between Government agencies. This appendix describes the general efforts being undertaken by the Federal Government to utilize online electronic regulatory docket capabilities, specifically the usage of www.Regulations.gov (Regulations.gov) and the Federal Docket Management System (FDMS) at www.FDMS.gov.

The central eRulemaking tool for Federal agencies is Regulations.gov. Launched in 2003, the website provides agencies with a platform to post final rules, proposed rules, requests for information, and other public documents in order to give the public an opportunity to review and comment on regulatory actions. There is a commenting feature on FederalRegister.gov which is integrated with existing MyFR and social media capabilities on the website to allow for more public interaction with the agency. The eRulemaking Program Management Office is hosted by the Department of Environmental Protection (EPA). The eRulemaking program offers an application programming interface (API) which connects outside applications to FDMS so interested individuals can both read regulatory information and write comments to be processed through FDMS. FDMS is the Government-wide system that provides agencies the ability to search, view, download, and review comments on rulemaking and non-rulemaking initiatives. FDMS also enables agency users to manage docket materials through the use of role-based access controls, workflow and collaboration processes, and comment management tools. Many departments and agencies have extensively used these tools to facilitate their regulatory activities. Many Federal agencies have used the system to great effect, posting large amounts of content and receiving tremendous input from the public on proposed regulatory action.

As part of the broader OMB effort to reduce reporting burden places on Federal agencies, OMB did not request this information in its annual E-Gov Act implementation data collection this year. To view proposed rules, requests for information, or other documents that Federal agencies have issued for public feedback, please view the Regulations.gov or FDMS websites.

APPENDIX F. NATIONAL ARCHIVES AND RECORDS ADMINISTRATION (NARA) RECORDKEEPING

Sections 207 (e) of the E-Gov Act (44 U.S.C. § 3501 note) requires agencies to adopt policies and procedures to ensure that chapters 21, 25, 27, 29, and 31 of title 44, United States Code, are applied effectively and comprehensively to Government information on the Internet and to other electronic records. NARA coordinates with OMB to implement OMB memorandum M-12-18: *Management Government Records Directive*, which requires that to the fullest extent possible, agencies eliminate paper and use electronic recordkeeping. Senior Agency Officials for Records Management are required by M-12-18 to report to NARA on agency progress in meeting the Directive goals, as well as on other significant records and information initiatives as defined by NARA.

NARA's process for overseeing agency compliance with recordkeeping procedures is through its the Records Management Oversight and Reporting Program, under the Office of the Chief Records Officer for the Federal Government. This program is responsible for monitoring compliance with records management regulations and implementation of NARA policies, guidance and other records management best practices by federal agencies. Under 44 U.S.C. 2904(c)(7) and 2906, NARA has the authority to conduct inspections or surveys of the records and records management practices of Federal agencies for the purpose of providing recommendations for improvements. The criteria for selecting agencies for inspection or records management program review include, but are not limited to, the results of an agency's annual records management self-assessment, the significance of certain records and the related business processes, the risk of improper management of records, and the presence of important issues that are relevant to management of Federal records in general.

As part of the broader OMB effort to reduce reporting burden places on Federal agencies, OMB did not request this information in its annual E-Gov Act implementation data collection this year. To view NARA's record of agency inspections, records management program reviews, surveys and assessments, and annual reporting, please view the program's website.

APPENDIX G. PRIVACY POLICY AND PRIVACY IMPACT ASSESSMENTS

Section 208(b) of the E-Gov Act (44 U.S.C. § 3501 note) requires agencies to conduct a privacy impact assessment before (1) developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or (2) initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons. In addition, and if practicable the E-Gov Act requires that agencies make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means. Individuals interested in reviewing agencies' compliance with the privacy provisions of the E-Gov Act should reference the privacy section of the annual FISMA report.

APPENDIX H. AGENCY IT TRAINING PROGRAMS

Section 209(b)(2) of the E-Gov Act (44 U.S.C. § 3501 note) requires agencies to establish and operate IT training programs. The Act states that such programs shall have curricula covering a broad range of information technology disciplines corresponding to the specific information technology and information resource management needs of the agency involved; be developed and applied according to rigorous standards; and be designed to maximize efficiency, through the use of self-paced courses, online courses, on-the-job training, and the use of remote instructors, wherever such features can be applied without reducing the effectiveness of the training or negatively impacting academic standards. This appendix describes select agency training programs for IT workforce. Agency IT workforce training is described below, with one paragraph highlighting a specific agency's accomplishments. The full list of activities can be found on the IT Dashboard.

DOD, DHS, and NIST collaborated to create the NIST Special Publication 800-18: *National Initiative for Cybersecurity Education Cybersecurity Workforce Framework*, which was published in August 2017. The document includes core elements of the DOD Cyber Workforce Framework (DCWF). DCWF qualification standards were internally matured and defined for the majority of the 53 cyber work roles. The remaining research will be completed in 2018. DCWF will enhance current cyber training and education in Military and Agency technical schoolhouses and online offerings. DCWF will also improve training effectiveness and cyber personnel readiness through innovative performance assessments.

DOC also focused on enhancing its cybersecurity awareness and training program in FY 2017. DOC implemented role-based Cyber Security Assessment and Management (CSAM) training to help standardize and increase CSAM usage within the agency. As part of DOC's goal to be a leader in cybersecurity training across the Federal Government, the agency hosted three quarterly cybersecurity technical workshops, which were attended by representatives of over 44 Governmental agencies. DOC also enhanced the authorizing official and system owner-training curriculum, and updated its cybersecurity workforce development policy to integrate training concepts identified in NIST SP 800-16. Finally, DOC expanded its security awareness campaign by delivering 21 cybersecurity instructor-led awareness training sessions addressing techniques to prevent phishing, social engineering and identity theft.

The National Science Foundation (NSF) required all staff to complete the 2017 Security and Privacy Awareness Training, which was developed internally to address IT security threats specific to NSF. The content includes relevant topics such as phishing prevention, personally identifiable information (PII) protection and safe file storage and transfer. The completion rate in 2017 was 99.97%. Additionally, all employees and managers who have elevated cyber security roles are assigned Insider Threat Awareness Training, utilizing content provided by the Defense Security Service.

In FY 2017, NARA offered its revamped Tier I Computer Based Training to better address emerging threats. As other emergent threats are recognized, the agency reviews and updates its multi-level Tier II training program for users with elevated security responsibilities

and other staff involved in Risk Management activities. Classroom instructions, along with on-site delivery of awareness training, were offered in the FY 2017 training cycle. Finally, FISMA-compliant IT security training is required at the time of on boarding and annually for all NARA staff (employees and contractors), along with training on protections for privacy-related information.

DOJ utilized its IT workforce training in FY 2017 to bring together IT professionals from across divisions to break down organizational silos and share knowledge. DOJ also successfully implemented standard frameworks, such as the NICE framework for cybersecurity, to better benchmark and coordinate IT employee development, and continued to implement the requirements of the Federal Cybersecurity Workforce Assessment Act. In addition, DOJ passed a 2017 GAO audit and created a Department-wide working group to identify and code all of its employee positions against the NICE 2.0 standard. The DOJ IT Flash Mentoring series continued to grow providing development and networking opportunities for the Department IT Community. Finally, DOJ's Office of the CIO continued to pilot a Skills Incentive Program that maps desired certifications and competencies to specific job functions and General Schedule grades. The objective is to regularly review and iterate the framework so that it evolves with the changing skill-type demands within the IT field. The end goal is for this to serve as a model for DOJ-wide IT workforce development.

ED on the other hand, in FY 2017 continued its efforts to deliver training and development opportunities to a more mobile workforce. Employees were provided access to virtual books through ED's learning management system. The books included a wide range of IT related training topics, including: IT security, project management, databases, operating systems, and networking. To enhance training efforts with remote staff, ED continued to use WebEx and remote presence software (video/audio broadcast). In addition, the agency modified its IT Security Role Base Training to encourage IT professionals to take training courses related to obtaining cyber security certifications. IT Security Role Based Training was assigned to 771 employees and 100% of the employees completed it. Cybersecurity and Privacy Awareness training was required of all ED employees and 100% of employees completed this training.

In FY 2017, the Department of Housing and Urban Development (HUD) completed its Enterprise-Wide Information Security Workforce Training Program Plan. This plan serves as HUD's solution to meet the advanced training needs of its security staff. HUD also conducted Information Security Continuous Monitoring training for all Information System Security Officer's (ISSO's). In addition, HUD administered an IT Specialist Skills Assessment as part of a Department-wide initiative to evaluate the skills of HUD's workforce. Also in 2017, the results of the FY 2016 Skills Assessment were published, which identified the skills that are considered to be most important and have the largest proficiency gaps. The objectives of the assessment included: (a) identifying skill gaps within the HUD IT workforce; (b) identifying training needs and providing recommendations on future trainings to be included in the HUD LEARN curriculum; and (c) comparing the results of the FY 2014 and FY 2016 IT Skills Assessment results to assess progress toward gap closure and the success of existing training.

The Environmental Protection Agency's (EPA) IT training program hosted 295 Instructor-led trainings in FY 2017. EPA has also partnered with an eLearning service provider

to provide 24/7 access to state-of-the art IT, project management, contracts management, leadership, compliance, and core competency learning assets across the enterprise. The eLearning provider recently added live simulations, real-time coaching and other enhancements to their learning programs for IT professionals. The EPA Office of Environmental Information also provided IT training programs that are delivered in both classroom settings and via virtual delivery methods. Finally, the EPA provided access to mandatory IT training for all contractors, grantees and students who have access to the Agency systems

The Office of the CIO at GSA (now GSA IT) provides in-person and online enterprise-wide training to GSA's 17,000+ staff to help improve their technical skills. In FY 2017, GSA held 80 instructor-led IT training courses. GSA also overhauled its privacy training offerings this year. Its mandatory privacy awareness training was designed for adult learning and focused on the concept of Controlled Unclassified Information (CUI) and the categories of personally identifiable information (PII) commonly collected, maintained or disseminated by GSA; three key aspects of the Privacy Act; five ways that employees can protect PII; and instructions on how to report a breach. In addition, GSA IT conducted an organization-wide introductory agile training and established a Leadership & Development steering committee to provide oversight for all training-related policies and processes. GSA IT also created in-house development opportunities by establishing an IT-specific rotational program, formalized a governance process for participating in external leadership programs and conferences, and began piloting different Massive Open Online Courses (MOOCs) for enterprise-wide use. Other agencies have consulted GSA to learn about migrating their e-mail to the cloud and implementing Software as a Service (SaaS) collaboration tools. GSA holds quarterly Interagency Center of Excellence meetings about these tools to discuss topics across agencies, including new features, demonstrations of applications, and upcoming conferences/events.

In FY 2017, employees at OPM took a wide range of IT courses via the OPM Learning Connection, which makes over 300 IT-related courses available to employees. Of these, 272 unique IT courses were completed throughout FY 2017. OPM's Office of the CIO acquired IT Infrastructure Library (ITIL) Foundation framework training classes, which were attended by OPM staff in FY 2017. The ITIL framework is designed to standardize the selection, planning, delivery, and support of IT services within OPM, which aligns IT services with agency needs. Class attendees were required to pass an ITIL Foundation certification test in order demonstrate their understanding of ITIL Foundation concepts. OPM's Office of the CIO also acquired Agile training classes "Agile and Scrum in a Day" and "Certified Scrum Product Owner." OPM staff attended these Agile and Scrum classes in FY 2017, which provide the foundation for OPM staff in understanding and putting into practice the Agile Scrum process from the perspective of the OPM Program Office organization responsibilities.

APPENDIX I. CROSSWALK OF E-GOV ACT REPORTING REQUIREMENTS

E-Government Act of 2002 Requirement	Location in E-Government Act Report to Congress
Sec. 101 (44 U.S.C. § 3606) – Provide a description of projects receiving E-Gov Funds in FY 2016, including funding allocations and results achieved.	Section I – E-Government Fund
Sec. 209 (44 U.S.C. § 3501 note) – Provide a summary of activities related to IT workforce policies, evaluation, training, and competency assessments.	Section II – Government-wide IT Workforce and Training Policies
Sec. 214 (44 U.S.C. § 3501 note) – Provide a summary of how IT is used to further the goal of maximizing the utility of IT in disaster management.	Section III – Disaster Preparedness
Sec. 216 (44 U.S.C. § 3501 note) – Provide a summary of activities on geographic information systems and initiatives, and an overview of the Geospatial Platform.	Section IV – Geospatial
Sec. 101 (44 U.S.C. § 3602(f)(9)) – Sponsor ongoing dialogue to encourage collaboration and enhance understanding of best practices and innovative approaches in acquiring, managing, and using information resources to improve the delivery of Government information and services to the public.	Appendix A - Enhanced Delivery of Information and Services to the Public
Sec. 202(b) (44 U.S.C. § 3501 note) – Develop performance measures.	Appendix B – Performance Integration
Sec. 202(d) (44 U.S.C. § 3501 note) – Ensure comparable accessibility to people with disabilities.	IT Dashboard
Sec. 202(e) (44 U.S.C. § 3501 note) – Engage the public in development and implementation of policies.	Appendix C – Government-Public Collaboration

E-Government Act of 2002 Requirement	Location in E-Government Act Report to Congress
Sec. 203 (44 U.S.C. § 3501 note) – Implement electronic signatures.	Appendix D – Credentialing Note: In an effort to reduce reporting burden on agencies, information for this appendix was not collected this year.
Sec. 204 (44 U.S.C. § 3501 note) – Oversee the development of a Federal Internet Portal.	IT Dashboard
Sec. 206 (44 U.S.C. § 3501 note) – Report to Congress agency compliance with electronic dockets for regulatory agencies. Ensure public websites contain electronic dockets for rulemaking.	Appendix E – E-Rulemaking Note: In an effort to reduce reporting burden on agencies, information for this appendix was not collected this year.
Sec. 207 (e) (44 U.S.C. § 3501 note) – Report on agency compliance with policies pertain to the organization and categorization of Government information, and agency compliance with establishing policies and procedures regarding recordkeeping.	Appendix F – National Archives Records Administration Recordkeeping Note: In an effort to reduce reporting burden on agencies, information for this appendix was not collected this year.
Sec. 207(f)(1)A(ii) (44 U.S.C. § 3501 note) – Report on agency compliance with requirements to make information available to the public under the Freedom of Information Act.	IT Dashboard
Sec. 207(f)(1)(A)(iv) (44 U.S.C. § 3501 note) – Report on agency compliance with requirements to provide an information resources strategic plan.	IT Dashboard
Sec. 207(f)(1)(B) (44 U.S.C. § 3501 note) – Report on agency compliance with developing goals to assist the public with navigating agency websites.	IT Dashboard

E-Government Act of 2002 Requirement	Location in E-Government Act Report to Congress
Sec. 207(g) (44 U.S.C. § 3501 note) – Develop a Government-wide repository and website for all Federally funded research and development.	IT Dashboard
Sec. 208(b) (44 U.S.C. § 3501 note) – Report on agency compliance with developing a privacy policy and conducting privacy impact assessments.	Appendix G – Privacy Policy and Privacy Impact Assessments Note: In an effort to reduce reporting burden on agencies, information for this appendix was not collected this year.
Sec. 209(b)(2) (44 U.S.C. § 3501 note) – Report on agency compliance with establishing information technology training programs.	Appendix H – Agency Information Technology Training Programs